

При формировании ТПУ Московской агломерации возможна планировка ТПУ в двух вариантах. Первый предусматривает создание «плоскостного» ТПУ со следующими мероприятиями: строительство и реконструкция в ТПУ объектов транспортного назначения («перехватывающие» парковки, отстойно-разворотные площадки, пассажирские платформы и т. д.); покрытие посадочных перронов навесами, защищающими пассажиров от атмосферных осадков; упорядочение объектов мелкорозничной торговли в ТПУ; создание пространственно-функциональной взаимосвязи между отдельными элементами ТПУ и т. д. Второй подход подразумевает строительство многоуровневых ТПУ, обеспечивающих комфортные условия пересадки с одного вида транспорта на другой (например, железная дорога – метрополитен) или в пределах транспортной сети одного вида транспорта (например, с одного железнодорожного направления на другое). Каждый уровень такого ТПУ имеет свою специализацию и объединяет все его основные элементы. Для обеспечения инвестиционной привлекательности такого объекта в составе ТПУ необходимо размещение коммерческих объектов. Вопрос размещения, состава и размера коммерческих площадей ТПУ должен прорабатываться с целью реализации основной его социальной задачи – обеспечения максимально комфортной пересадки пассажиров с минимальными затратами времени.

При формировании ТПУ для обеспечения удобной и комфортной пересадки пассажиров необходимо изменение существующего взаимного расположения устройств по обслуживанию пассажиров. Оптимизация структуры площадей в целях максимизации доходности ТПУ при одновременном выполнении условий удовлетворения потребности пользователей к обслуживанию позволит: определить необходимые размеры операционных площадей; увеличить до максимально возможного уровня доли коммерческих площадей; снизить до минимально необходимого уровня доли служебных площадей, выделенных для служб ТПУ и для организаций, занимающих территорию на безвозмездной основе.

Оценку эффективности планировочных решений, формируемых ТПУ и ТПК в Московской агломерации, можно провести с помощью имитационного моделирования на основе данных о пассажиропотоках методом многокритериальной системы оценок, в котором каждому критерию работы ТПУ и ТПК (длина очереди, общее время пересадки, кратчайшее расстояние пересадки, состав и размер проектируемых площадей ТПК и т. д.) присваивается коэффициент, который соответствует «весу» данного параметра в итоговом значении оценки эффективности рассматриваемого варианта.

Создание сети мультимодальных ТПУ улучшит уровень транспортного обслуживания мегаполиса; вызовет увеличение доли населения, пользующегося общественным транспортом; сократит время, затрачиваемое пассажирами на поездки, что позволит повысить уровень социального обслуживания жителей города Москвы и его пригородов, сделать их привлекательнее для финансовых вложений; улучшить экологию.

УДК 656.259.4

## **ИССЛЕДОВАНИЕ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ТЕХНОЛОГИИ ЗАЩИТЫ ГОРОДСКОЙ РЕЛЬСОВОЙ ТРАНСПОРТНОЙ СИСТЕМЫ СИГНАЛОВ**

*ВАН ЦЗИНЬЛАНЬ*

*Гуанчжоуский железнодорожный профессионально-технический колледж,  
Китайская Народная Республика*

*ЧЖАН ЧЖЭНСИНЬ*

*Пекинский информационный профессионально-технический колледж,  
Китайская Народная Республика*

*ВАН ЦЗЯНЬ*

*Пекинский университет транспорта, Китайская Народная Республика*

Городская рельсовая транспортная система сигналов характеризуется сложной структурой сети, различными уровнями безопасности, сложной конфигурацией сетевого управления, что вызывает необходимость разработки единой стратегии контроля и эксплуатационных требований безопасности, а также централизованного интеллектуального управления рисками по информационной без-

опасности. Поэтому проведение исследования в области информационной безопасности и технологии защиты городской рельсовой транспортной системы сигналов имеет очень важное практическое значение.

Проблема безопасности в области сигналов рельсового транспорта сосредоточена на уровне, называемом «Safety», который в соответствии с европейским стандартом EN50126 определяется как «freedom from unacceptable risk of harm». При этом следует также рассматривать в данном контексте и проблему информационной безопасности (Security), которой в последние годы активно занимается промышленный контроль, для выяснения причин аварий рельсового транспорта. Система сигналов рельсового транспорта имеет характеристики быстрого перемещения контролируемых поездов, управления распределением на большие расстояния управляющего оборудования и режима беспроводной связи между транспортным средством и землей. По сравнению со стандартными характеристиками статической проводной связи традиционной системы промышленного управления система сигналов рельсового транспорта более уязвима для целенаправленных атак извне и также имеет свою специфику и практические характеристики.

Следует отметить, что размещение оборудования рельсовой транспортной системы сигналов имеет различные характеристики из-за передачи информации на большие расстояния и расположения на разных станциях, центрах управления и т. п. Сетевая и системные сети не подключены к Интернету. Однако имеется проводной доступ к кабелю в любых местах, что делает сетевые атаки возможными, и в то же время, если работа системы, техническое обслуживание, управление не стандартизованы, неправильное использование мобильной памяти на терминале ПК также вызовет сбой в системе. Поэтому для обеспечения безопасности высокоскоростного движения поездов наземная сигнальная система и система сигналов транспортного средства должны обмениваться данными. Двусторонняя беспроводная передача, охватывающая всю линию, и полностью открытое пространство передачи приводят к множеству угроз информационной безопасности. Так, в процессе движения поезда большое количество данных, связанных с его безопасностью, передается в реальном времени между транспортным средством и наземным оборудованием и устройствами, что может привести к нарушению передачи сигнала и, как следствие, к техногенным авариям. В то же время в процессе движения поезда необходимо обрабатывать и управлять значительными массивами динамических и статических данных, что также является важным аспектом безопасности данных железнодорожной сигнальной системы.

Анализ структуры информационной безопасности рельсовой транспортной системы сигналов показал, что необходимо создать всеобъемлющую структурную систему (рисунок 1), включающую политику безопасности, управление безопасностью и технологии безопасности.

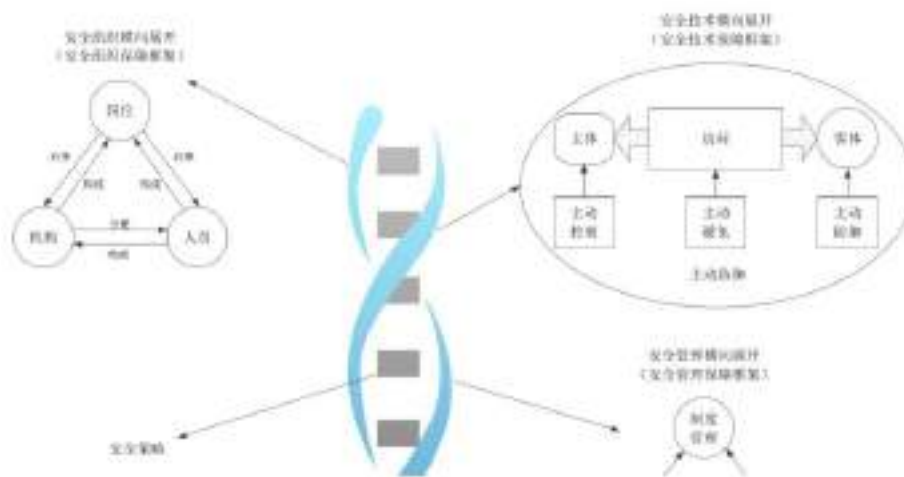


Рисунок 1 – Система структуры информационной безопасности рельсовой транспортной системы сигналов

Вышеназванные проблемы в процессе проектирования и применения аппаратного и программного обеспечения рельсовой транспортной системы сигналов пока еще не полностью изучены. При этом основная проблема при передаче сигналов, управлению ими и обслуживанию всё еще находится на уровне совместной работы безопасной эксплуатации (Safety) и других связанных с этим операционных целей (эффективность транзита, экономическая эффективность и т. д.). В настоящее

время не удалось установить полную эффективную линию безопасности конкретно для уровня информационной безопасности (Security). Кроме того, отсутствие соответствующих стандартов и норм в области информационной безопасности, недостаток соответствующего моделирования, тестирования и анализа условий окружающей среды еще больше усилили глубокие противоречия между нынешней постепенно возрастающей осведомленностью о безопасности (Security) и трудно выполнимыми условиями по её совершенствованию.

Структура информационной безопасности (см. рисунок 1) может непрерывно улучшаться, развиваться и удовлетворять требованиям мер безопасности с изменениями в применении рельсовой транспортной системы сигналов, постоянно обнаруживать новые проблемные факторы, приводящие к угрозам и рискам (таблица 1).

Таблица 1 – Краткая характеристика требований по обеспечению безопасности

Классификационная градация структуры по обеспечению безопасности	Краткая характеристика
Организации	<ul style="list-style-type: none"> <li>– создание агентств безопасности информационных систем;</li> <li>– создание позиций безопасности в соответствии с требованиями безопасности системы;</li> <li>– обучение персонала по обеспечению безопасности и повышение его квалификации</li> </ul>
Технологии	<ul style="list-style-type: none"> <li>– использование технологий аутентификации и авторизации, шифрования и защиты целостности;</li> <li>– проведение проверки подлинности и управление доступом;</li> <li>– шифрование информации для предотвращения ее раскрытия и несанкционированного использования информации</li> </ul>
Управление	<ul style="list-style-type: none"> <li>– обеспечение системного и технического управления;</li> <li>– организация управления персоналом;</li> <li>– внедрение ряда внутренних правил и положений, а также стандартизация использования продуктов безопасных технологий;</li> <li>– проверка и оценка труда персонала по обеспечению безопасности и его обучение</li> </ul>

Помимо вышеизложенного необходимо улучшить защиту системы от атак посредством проверки и обнаружения вторжений, а также других средств, позволяющих выполнить оценку последствий и принятия мер по предотвращению ущерба. В связи с этим целесообразно выявить причины уязвимости информационной безопасности городской рельсовой транспортной системы сигналов, основанной на коммуникационной системе управления поездами CBTC (Communication – Based Train Control) и соответствующей стандарту IEEE1474, который определяет её функции с помощью подсистемы передачи данных DCS (Data Communication Subsystem) и позволяет осуществлять двустороннюю передачу данных большого объема между оборудованием поездов и железнодорожным оборудованием. Система CBTC состоит из трех частей: наземной кабельной сети, кабельной сети на поезде, сети беспроводной связи между транспортными средствами и землей (рисунок 2).

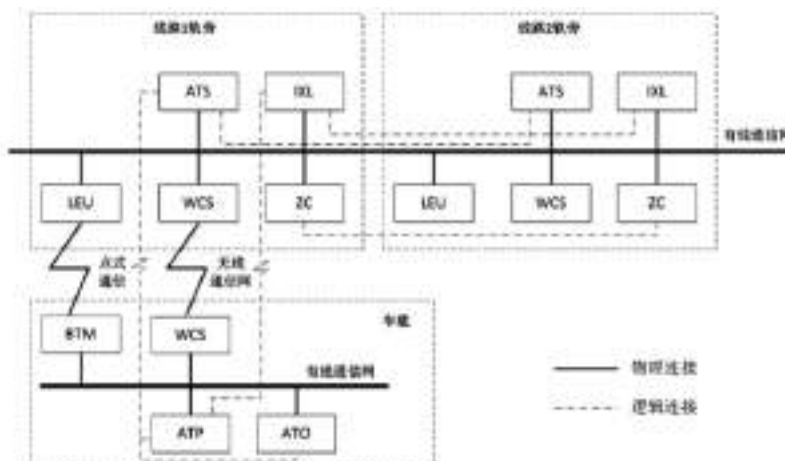


Рисунок 2 – Структура информационной безопасности рельсовой транспортной системы сигналов

Схема, приведенная на рисунке 2, позволяет центру управления вычислять и регулировать максимальное тормозное расстояние поезда согласно информации о скорости и местоположении в режиме реального времени для достижения непрерывного автоматического управления поездами. Рассматри-

ваемая система DCS – это широкополосная система связи, основанная на стандарте проводной сети IEEE802.3 и на стандарте беспроводной сети IEEE802.11g для использования беспроводной связи.

В связи с высокой пропускной способностью и благодаря технологии Ethernet проблема потери пакетов данных и место задержки системы СВТС в основном сосредоточены между транспортными средствами и землей. Тем не менее для обеспечения наблюдения в реальном времени, надежности и удобства использования связи сигнального оборудования в сети передачи данных сигнальной системы DCS не использованы меры для информационной безопасности, а также не обеспечена особая защита по характеристикам применения городских рельсовых транспортных сигналов. Открытость беспроводной сети и недостатки самого строения беспроводной сети приводят к тому, что в системе появляются риски, такие как вмешательство и атаки. Это становится самой большой угрозой информационной безопасности системы СВТС. Основными причинами этих рисков являются беспроводные помехи, отказ в обслуживании, беспроводное вторжение и беспроводной обман. Из-за популярности интеллектуальных терминалов и открытого источника инструментов беспроводных атак уязвимость беспроводной сети СВТС экспоненциально масштабируется.

Таким образом, существует немало проблем в таких аспектах, как стратегия защиты и механизм ее организации в информационной безопасности рельсовой транспортной системы сигналов. Поэтому авторами статьи предлагаются практические рекомендации, приведенные в таблице 2.

Таблица 2 – Практические рекомендации в организации информационной безопасности

Направление	Краткая характеристика
Активная технология защиты	
Вертикальная стратификация	Разделение управления и контроля от сети
Горизонтальное разделение	Изоляция различных подсистем от сети
Пограничный контроль, внутреннее тестирование и демонстрация различных подсистем	Реализация внутреннего тестирования сетевого потока и тестирование для обнаружения вторжения в режиме реального времени
	Мониторинг оборудования, бизнес-процессов и т. п.
Двухсторонняя аутентификация системного улучшения	Многоуровневое раннее предупреждение и контроль рисков
	Защита информационной безопасности городской рельсовой транспортной системы сигналов
Технология контроля безопасности доступа к информации	
Ограничение несанкционированного использования системы сигналов доступа информации	Обеспечение эффективного использования и управления данными в пределах законодательства
	Идентификация и аутентификация личности, контроль прав и аудит безопасности
Проверка системных полномочий	Применение методов мониторинга, блокировки и аудита для анализа несанкционированной работы системы
Разделение системных прав	Минимизация и техническое применение проверки компетенции

Таким образом, интеграция новых сетевых технологий и технологий управления позволяет использовать программное обеспечение для определения сети SDN, делает возможным применение политики безопасности в различных сетевых устройствах для достижения управления безопасностью во всей сетевой связи. Поэтому при разработке интегрированной с контролем сигнальной системы нового типа обеспечивается высокий уровень безопасности дорожного движения и реализуется ее глубокая защита.

УДК 656.052 : 656.224

## ОСНОВНЫЕ ТЕНДЕНЦИИ И ОСОБЕННОСТИ ПРИГОРОДНЫХ ПЕРЕВОЗОК НА ЖЕЛЕЗНОДОРОЖНОМ ТРАНСПОРТЕ В КРУПНЕЙШИХ АГЛОМЕРАЦИЯХ ЕВРОПЫ В КОНЦЕ XIX–XX вв.

Т. А. ВЛАСЮК

*Белорусский государственный университет транспорта, г. Гомель*

В Европе в конце XIX в. железнодорожный транспорт начал активно развиваться и связывал центр городов с пригородными районами, что способствовало росту числа промышленных предприятий в окрестностях городов и за их пределами. Например, в 1851–1867 годах в Париже была проложена сеть железных дорог для перевозки пассажиров и грузов, которая проходила через новые территории, присоединенные к Парижу в 1860 году. Появление маятниковой миграции произвело значительное воздействие на жизненный уклад населения и позволило «вырасти» не только